



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/822,219

04/09/2004

Atam P. Dhawan

436/8

1317

27538

7590

12/05/2006

KAPLAN GILMAN GIBSON & DERNIER L.L.P.
900 ROUTE 9 NORTH
WOODBIDGE, NJ 07095

EXAMINER

BAUM, RONALD

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 12/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/822,219	Applicant(s) DHAWAN, ATAM P.	
	Examiner Ronald Baum	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 August 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 7-13, 20-26 is/are allowed.
- 6) ☒ Claim(s) 1-6, 14-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 29 August 2006.
2. Claims 1-26 are pending for examination.
3. Claims 1-6, 14-19 are rejected.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. The Claims 7-13, 20-23 rejections under 35 U.S.C. 112, second paragraph, is withdrawn.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-3, 6, 14-16, 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Zeng et al, U.S. Patent No. 6,505,299 B1.

6. As per claim 1; "A method, comprising:

converting original data into

a plurality of sub-bands using

wavelet decomposition [Abstract, col. 1, lines 10-col. 3, line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13, 16, 17, whereas the use of ‘... grouping a set of transform coefficients from a special frequency subband and shuffling the transform coefficients ...’ (i.e., col. 3, lines 24-36), clearly encompasses the claimed limitations, as broadly interpreted by the examiner, insofar as post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing.];

encrypting at least one of the sub-bands using

a key to produce

encrypted sub-band data [Abstract, col. 1, lines 10-col. 3, line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13, 16, 17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic (i.e., col. 3, lines 24-36) encryption/decryption (key oriented) functions, clearly encompasses the claimed limitations, as broadly interpreted by the examiner.]; and

transmitting the encrypted sub-band data to

a recipient separately from

the other sub-bands [Abstract, col. 1, lines 10-col. 3, line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13, 16, 17, whereas the use of cryptographic encryption/decryption (key oriented) functions on post wavelet decomposed sub-band separated data packets, subsequently transferred

across the Internet (i.e., a packet oriented, multi-path routed network), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.].”.

And further as per claim 14, this claim is an apparatus claim for limitations from the method claim 1 above, and is rejected for the same reasons provided for the claim 23 rejection; “An apparatus including a processor operating under the instructions of a software program, the software program causing the apparatus to perform actions, comprising: converting original data into a plurality of sub-bands using wavelet decomposition; encrypting at least one of the sub-bands using a key to produce encrypted sub-band data; and transmitting the encrypted sub-band data to a recipient separately from the other sub-bands.”.

7. Claim 2 *additionally recites* the limitations that; “The method of claim 1, further comprising
embedding at least one message in
the at least one sub-band prior to
the encryption step.”.

The teachings of Zeng et al (Abstract, col. 1, lines 10-col. 3, line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13, 16, 17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic (i.e., col. 3, lines 24-36) encryption/decryption (key oriented) functions (insofar as the transform coefficient map is inherently a signature (a digital signature) for the

Art Unit: 2136

data group/sub-band it is associated with), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 15, this claim is an apparatus claim for limitations from the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection; “The apparatus of claim 14, further comprising embedding at least one message in the at least one sub-band prior to the encryption step.”.

8. Claim 3 *additionally recites* the limitations that; “The method of claim 2, wherein the at least one message is at least one of
- hashed,
 - digitally signed for, and
 - encrypted
- prior to embedding the at least one message in
- the at least one sub-band.”.

The teachings of Zeng et al (Abstract, col. 1, lines 10-col. 3, line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13, 16, 17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (key oriented) functions (insofar as the transform coefficient map is inherently a signature (a digital signature) for the data group/sub-band it is associated with), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 16, this claim is an apparatus claim for limitations from the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection; “The apparatus of claim 15, wherein the at least one message is at least one of hashed, digitally signed for, and encrypted prior to embedding the at least one message in the at least one sub-band.”.

9. Claim 6 *additionally recites* the limitations that; “The method of claim 1, further comprising:

encrypting a plurality of the sub-bands using
respective secret keys to produce
respective encrypted sub-band data,
each secret key being the same or different from
one of more of the respective secret keys; and
transmitting the respective encrypted sub-band data over
at least some differing routes of
a packet-switched network to
the recipient.”.

The teachings of Zeng et al (Abstract, col. 1, lines 10-col. 3, line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13, 16, 17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (symmetric/secret key oriented) functions,

Art Unit: 2136

subsequently transferred across the Internet (i.e., a packet oriented, multi-path routed network), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 19, this claim is an apparatus claim for limitations from the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection; “The apparatus of claim 14, further comprising: encrypting a plurality of the sub-bands using respective secret keys to produce respective encrypted sub-band data, each secret key being the same or different from one of more of the respective secret keys; and transmitting the respective encrypted sub-band data over at least some differing routes of a packet-switched network to the recipient.”.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 4,5,17,18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zeng et al, U.S. Patent No. 6,505,299 B1, as applied to claim 1,14 above and further in view of below

It is noted that Zeng et al, (U.S. Patent No. 6,505,299 B1) does not disclose in the image coding system/method the specific type of encryption used other than to distinguish said encryption as requiring a minimal relatively processing capability. However, the examiner asserts that it would have been obvious to one ordinary skill in the art at the time the invention was made to use generally accepted state of the art encryption cryptographic functionality at the time of the invention. Typically this would encompass symmetric key cryptographic functionality (i.e., secret key encryption such as DES, etc.,) with accompanying public key cryptographic functionality (i.e., public key encryption such as used in PGP authentication, etc.,). A recitation directed to the manner in which a claimed apparatus is intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)).

11. Claim 4 *additionally recites* the limitations that; "The method of claim 3, wherein
a private key is employed when
the at least one message is digitally signed for, and
a secret key is employed when
the at least one message is encrypted."

The teachings of Zeng et al (Abstract, col. 1, lines 10-col. 3, line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13, 16, 17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (key oriented) functions (insofar as the transform coefficient map is inherently a signature (a digital signature) for the data group/sub-band it is

Art Unit: 2136

associated with), clearly encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 17, this claim is an apparatus claim for limitations from the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection; “The apparatus of claim 16, wherein a private key is employed when the at least one message is digitally signed for, and a secret key is employed when the at least one message is encrypted.”.

12. Claim 5 *additionally recites* the limitations that; “The method of claim 1, wherein the at least one message is
- a digital signature,
- which is transmitted to
- the recipient to
- verify the integrity of
- the encrypted sub-band data.”.

The teachings of Zeng et al (Abstract, col. 1, lines 10-col. 3, line 63, figures 1-17 and associated descriptions, and more particularly figures 11-13, 16, 17, whereas the post wavelet sub-band separation and resulting sub-band transform coefficients subsequent processing encompassing the use of cryptographic encryption/decryption (key oriented) functions (insofar as the transform coefficient map is inherently a signature (a digital signature) for the data group/sub-band it is associated with), subsequently transferred across the Internet (i.e., a packet oriented, multi-path routed network that encompasses packet authentication at appropriate OSI layers), clearly

Art Unit: 2136

encompasses the claimed limitations, as broadly interpreted by the examiner.) suggest such limitations.

And further as per claim 18, this claim is an apparatus claim for limitations from the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection; “The apparatus of claim 14, wherein the at least one message is a digital signature, which is transmitted to the recipient to verify the integrity of the encrypted sub-band data.”.

Allowable Subject Matter

13. Claims 7-13, 20-26 are allowed.

14. As per claim 7; “A method, comprising:

permitting a source entity to make a protocol selection concerning

(i) parameters of a wavelet decomposition process to which

original data are to be subject to

convert the original data into a plurality of sub-bands, and

(ii) parameters of an encryption process to which

at least one of the sub-bands is to be subject to

produce respective encrypted sub-band data; and

permitting the source entity to select

a respective security level to be associated with

the respective encrypted sub-band data;

comparing at least one of
the protocol selection and
selected security level(s)
with a database containing data concerning at least one of
(i) a probability that the encrypted sub-band data
may be broken given the protocol selection,
(ii) an association between
security levels and
protocol selections; and
advising the source entity to select at least one of
a different security level and
a different protocol
when a result of the comparison indicates
a ~~relatively high~~ probability that the encrypted sub-band data may be broken
exceeds a predetermined probability.".

15. As per claim 8; "The method of claim 7, wherein the protocol selection further includes at least one of: (i) parameters of a hashing process to which at least one message is to be subject prior to embedding the at least one message in one or more of the sub-bands, (ii) parameters of a digital signature to which the at least one message is to be subject prior to embedding the at least one message in one or more of the sub-bands, (iii) parameters of an encryption process to which the at least one message is to be subject prior to embedding the at least one message in one or

more of the sub-bands, and (iv) aspects of nodes of a packet-switched network through which the respective encrypted sub-band data are to traverse for transmission to a recipient.”.

16. As per claim 9; “The method of claim 7, further comprising: converting the original data into a plurality of sub-bands using the selected parameters of the wavelet decomposition process; encrypting at least one of the sub-bands to produce encrypted sub-band data using the selected parameters of the encryption process; and transmitting the encrypted sub-band data to the recipient as one or more separate packets from the other sub-bands.”.

17. As per claim 10; “The method of claim 9, further comprising: encrypting a plurality of the sub-bands using respective secret keys to produce respective encrypted sub-band data, each secret key being the same or different from one of more of the respective secret keys; and transmitting the packet(s) of the respective encrypted sub-band data over at least some differing routes of the packet-switched network to the recipient.”.

18. As per claim 11; “The method of claim 9, further comprising routing the packet(s) of the encrypted sub-band data to the recipient over trusted nodes of a packet-switched network, each trusted node having a node security level for comparison with the security level(s) associated with the respective encrypted sub-band data, wherein each packet may only be routed through a trusted node having a node security level equal to or higher than the security level associated with the encrypted sub-band data.”.

Art Unit: 2136

19. As per claim 12; “The method of claim 11, wherein at least one of: the node security levels of the trusted nodes are time variant in response to network conditions; and each node is capable of changing its security level in response to the network conditions.”.

20. As per claim 13; “The method of claim 11, further comprising merging two or more packets of the respective encrypted sub-band data into one or more further packets within a trusted node having a security level equal to or higher than the security level associated with the encrypted sub-band data.”.

21. As per claim 20; “An apparatus including a processor operating under the instructions of a software program, the software program causing the apparatus to perform actions, comprising:
permitting a source entity to make a protocol selection concerning

(i) parameters of a wavelet decomposition process to which
original data are to be subject to

convert the original data into a plurality of sub-bands, and

(ii) parameters of an encryption process to which
at least one of the sub-bands is to be subject to

produce respective encrypted sub-band data; and

permitting the source entity to select

a respective security level to be associated with
the respective encrypted sub-band data;

comparing at least one of

the protocol selection and
selected security level(s)
with a database containing data concerning at least one of
(i) a probability that the encrypted sub-band data
may be broken given the protocol selection,
(ii) an association between
security levels and
protocol selections; and
advising the source entity to select at least one of
a different security level and
a different protocol
when a result of the comparison indicates
a ~~relatively high~~ probability that the encrypted sub-band data may be broken
exceeds a predetermined probability.".

22. As per claim 21; "The apparatus of claim 20, wherein the protocol selection further includes at least one of: (i) parameters of a hashing process to which at least one message is to be subject prior to embedding the at least one message in one or more of the sub-bands, (ii) parameters of a digital signature to which the at least one message is to be subject prior to embedding the at least one message in one or more of the sub-bands, (iii) parameters of an encryption process to which the at least one message is to be subject prior to embedding the at least one message in one or more of the sub-bands, and (iv) aspects of nodes of a packet-

Art Unit: 2136

switched network through which the respective encrypted sub-band data are to traverse for transmission to a recipient.”.

23. As per claim 22; “The apparatus of claim 20, further comprising: converting the original data into a plurality of sub-bands using the selected parameters of the wavelet decomposition process; encrypting at least one of the sub-bands to produce encrypted sub-band data using the selected parameters of the encryption process; and transmitting the encrypted sub-band data to the recipient as one or more separate packets from the other sub-bands.”.

24. As per claim 23; “The apparatus of claim 22, further comprising: encrypting a plurality of the sub-bands using respective secret keys to produce respective encrypted sub-band data, each secret key being the same or different from one of more of the respective secret keys; and transmitting the packet(s) of the respective encrypted sub-band data over at least some differing routes of the packet-switched network to the recipient.”.

25. As per claim 24; “A system, comprising:

a source entity operable to:

(i) convert original data into

a plurality of sub-bands using

a wavelet decomposition process,

(ii) encrypt at least one of the sub-bands to produce

encrypted sub-band data, and

(iii) transmit one or more packets of the encrypted sub-band data to
a recipient over a packet-switched network separately from
the other sub-bands; and
a plurality of trusted nodes within the packet-switched network,
each trusted node having
a node security level for comparison with
a security level associated with
the encrypted sub-band data,
wherein each packet may only be routed through a trusted node having
a node security level
equal to or higher than
the security level associated with
the encrypted sub-band data.”.

26. As per claim 25; “The system of claim 24, wherein at least one of:
the node security levels of the trusted nodes are
time variant in response to
network conditions; and
each node is capable of
changing its security level in response to
the network conditions.”.

27. As per claim 26; “The system of claim 24, wherein at least some of the trusted nodes are operable to

merge two or more packets of the encrypted sub-band data into

one or more further packets

when the given trusted node has

a security level equal to or higher than

the security level associated with

the encrypted sub-band data.”.

Response to Amendment

28. As per applicant’s argument concerning the lack of teaching by Zeng et al of ‘separate’ sub-channel transmission of at least an encrypted and other sub-band data, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive.

At the very least, the image space-frequency transform to generate a transform coefficient map, whereas said map is encrypted using at least the technique of grouping a set of transform coefficients from a spatial frequency sub-band and shuffling the transform coefficients within the group (i.e., col. 3, lines 24-53), clearly encompasses the ‘separate’ and encrypted sub-band aspects of the claim.

Also, the examiner broadly interprets the applicant’s use of the phrase ‘... at least one of the sub-bands ...’ in the context of the exclusion of the entire group of sub-bands such that if ‘all’ are encrypted, then when ‘all’ are subsequently forwarded across a network/communications channel, then inherently, there would be no accompanying non-

Art Unit: 2136

encrypted sub-channel to be sent. Nowhere in the claim language does the recitation of a requirement for an explicit claiming of the differentiation aspect concerning the various delineations of 'at least one ...' versus a requirement that '... but not all ...' appear; just the broad 'at least one ...' per se. Therefore, the various Zeng et al sub-band components construction, as being *broadly interpreted by the examiner*, as per the claim language, would therefore be applicable in the rejection, such that the rejection support references collectively encompass the said claim limitations in their entirety.

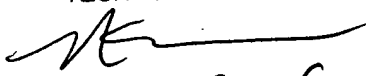
Conclusion

29. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


11/29/06

Ronald Baum

Patent Examiner

